IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 1:17-CR-00154 (TSE)
	)	
KEVIN PATRICK MALLORY,	)	
	)	
Defendant	)	

GOVERNMENT'S POSITION WITH RESPECT TO SENTENCING

The United States, by and through undersigned counsel, hereby files its position on sentencing. The United States has no objections to and does not dispute any facts or factors material to sentencing in the presentence report ("PSR"). For the reasons stated below, the Court should sentence Defendant Kevin Patrick Mallory to life imprisonment, which is a sentence consistent with the guidelines recommendation. It is also a sentence that is commensurate with Defendant's betrayal in this case. The Defendant betrayed the oaths that he took when he was employed by both the Central Intelligence Agency ("CIA") and the Defense Intelligence Agency ("DIA"). He betrayed the promises that he made in multiple non-disclosure agreements with both agencies to protect classified information. And he betrayed his obligations as a former handler of human assets to ensure that individuals who agree to help our government are not potentially exposed to harm.

I. INTRODUCTION

In July 2017, a grand jury returned an indictment charging Defendant with conspiracy to deliver, delivering, and attempting to deliver national defense information ("NDI") to the

Government of the People's Republic of China, and representatives, officers, agents, employees, subjects, and citizens thereof, in violation of 18 U.S.C. § 794, and one count of making materially false statements to special agents for the Federal Bureau of Investigation ("FBI"), in violation of 18 U.S.C. § 1001(a)(2). Dkt. No. 34.

Trial began on May 29, 2018. After an eight-day trial, the jury returned a verdict of guilty on all counts.[1] The Court scheduled sentencing for September 21, 2018.

II. A LIFE SENTENCE IS APPROPRIATE

A. Applicable Law and Guidelines Calculation

The advisory guideline range, as calculated pursuant to the U.S. Sentencing Guidelines ("USSG") is not binding upon the Court and instead constitutes a "starting point and initial benchmark" in the sentencing analysis. *Gall v. United States*, 552 U.S. 38, 49-50 (2007). Nonetheless, "a court of appeals may apply a presumption of reasonableness to a sentence imposed by a district court within a properly calculated guideline range . . . ." USSG Manual, published November 1, 2016, at 15 (citing *Rita v. United States*, 551 U.S. 338 (2007)). After ensuring that the advisory guideline range is properly calculated, the Court must consider whether a sentence within that range serves the factors and purposes set forth in 18 U.S.C. § 3553(a). *See United States v. Moreland*, 437 F.3d 424, 432 (4th Cir. 2006). If it does not, the Court must determine whether grounds for a departure exist under the guidelines or pertinent case law and apply them,

[1] The Court subsequently granted in part Defendant's Rule 29 motion and ordered acquittal on Counts Two (transmission of NDI) and Three (attempted transmission of NDI). Dkt. 201. The government's motion for reconsideration remains pending. However, regardless of the outcome of the government's motion, as is discussed below, because Defendant's conviction on Count One stands, the guidelines calculation is the same regardless of the outcome of the government's motion. Moreover, the conduct underlying the dismissed counts is something the Court can (and should) consider in fashioning Defendant's sentence. *See United States v. Watts*, 519 U.S. 148 (1997); *United States v. Carter*, 300 F.3d 415, 425-26 (4th Cir. 2002), *cert. denied*, 537 U.S. 1181 (2003); USSG § 1B1.3, comment, back'g; USSG 1B1.4.

as appropriate. *Id.*; *United States v. Tucker*, 473 F.3d 556, 560-61 (4th Cir. 2007) (consider departure ground before imposing variance). If, following that analysis, the Court still deems a sentence within the advisory guidelines range to be inadequate, the Court may further vary, above or below, that advisory range until it reaches a sentence that best serves the statutory sentencing factors and purposes. *See Moreland*, 437 F.3d at 432. Finally, the Court must state its reasons for imposing such a sentence, taking care to explain the reasons for any departure or variance. *Id.*; *see also* 18 U.S.C. § 3553(c)(2).

In this case, there is no advisory range. Rather, a calculation of an advisory sentence, pursuant to the Guidelines, results in a calculation of lifetime imprisonment. Defendant's convictions at trial for transmitting, attempting, and conspiring to transmit United States NDI classified at the SECRET and TOP SECRET levels and his failure to accept responsibility for his offenses result in a base offense level of 42 under USSG § 2M3.1. Even with the subsequent acquittal on Counts Two and Three of the Indictment (transmitting and attempting to transmit NDI), the remaining conviction for conspiracy to transmit NDI, including information classified at the TOP SECRET level, results in the same base offense level of 42 under USSG § 2M3.1. In addition, Defendant is subject to two enhancements based on the underlying facts of this case: (1) abuse of a position of trust, and (2) obstruction of justice.

Courts in this district have applied the abuse of position of trust enhancement to individuals who worked for the U.S. government and who violated the Espionage Act. *See, e.g.*, *United States v. Ford*, 288 F. App'x. 54, 61 (4th Cir. 2008) (No error in application of abuse of position of trust enhancement for 18 U.S.C. § 793 conviction because defendant's "abuse of his position of public trust contributed significantly to his commission of the offense. [The defendant] simply would not have been able to commit the offense of retaining classified documents without permission if he

had not held a top secret security clearance. . . ."); *United States v. Pitts*, 973 F. Supp. 576, 584 (E.D. Va. 1997) (Ellis, J) (increasing abuse of position enhancement by one additional level for former FBI agent convicted of violating 18 U.S.C. § 794 who "held a special position of awesome responsibility and trust [and] was supposed to safeguard this nation from foreign espionage activity" but who "[i]nstead . . . betrayed his country by engaging in the very activity that he was sworn to protect the nation against"), *aff'd*, 176 F.3d 239, 245 (4th Cir. 1999) (affirming district court's enhancement where "abuse of trust was extraordinary"). As discussed below in § II.B.2.a, Defendant used the prior access he had to highly sensitive NDI as a result of his former position of trust and TOP SECRET security clearance to commit these crimes.

The Guidelines also provide for a two-level enhancement for obstruction of justice. *See* USSG § 3C1.1. This enhancement applies for a number of reasons, including Defendant's destruction of the hard copies of the NDI at issue, concealment of the SD card containing the scanned NDI, and his false statements to FBI special agents.[2] *See* USSG, § 3C1.1, Application Note 4(D) (enhancement applies in cases where a defendant engages in "destroying or concealing or directing or procuring another person to destroy or conceal evidence that is material to an official investigation or judicial proceeding (e.g., shredding a document…)"); *id.* at Application Note 4(G) (enhancement applies where a defendant provided "a materially false statement to a law enforcement officer that significantly obstructed or impeded the official investigation or prosecution of the instant offense").

Combined with the abuse of a position of trust, the obstruction of justice sentencing enhancement increases Defendant's offense level to 46. Thus, even with Defendant having no

[2] To this day, the FBI does not have a clear idea as to what information Defendant gave to the Chinese government during his two trips to the PRC precisely because Defendant lied repeatedly during his May 24, 2017 interview with FBI special agents.

prior criminal history, placing him in Category I under the Guidelines, the seriousness of the crime, the involvement of TOP SECRET information, and these two enhancements result in Defendant's advisory guidelines range falling above the topmost tier of the Sentencing Table. *See* USSG Sentencing Table. Therefore, the Guidelines calculation recommends lifetime imprisonment. *See id.* (top offense level of 43 listing life in prison as advisory sentence). Given the facts of this case, this is the appropriate sentence.

B. 18 U.S.C. § 3553(a) Factors Support a Life Sentence

In addition to the Guidelines range, the factors for the district court to consider at sentencing include: (1) the history and characteristics of the defendant; (2) the nature and circumstances of the offense; (3) the important need for the sentence to reflect the seriousness of the crime and deter future criminal conduct; and (4) the need to avoid unwarranted sentencing disparities. 18 U.S.C. § 3553(a).

1. *History and characteristics of Defendant*

Defendant is a 61-year-old former intelligence officer, having worked as a covert case officer for the CIA in the 1990s and a senior intelligence officer for the DIA in the early 2000s. Defendant returned to the CIA as a contractor from 2010-2012.

Defendant was a seasoned intelligence professional who understood the importance of safeguarding classified national defense information, as well as the consequences—both personally and for our country—for failing to do so. In his positions within the United States Intelligence Community ("USIC"), Defendant held a TOP SECRET//SCI security clearance. "SCI" stands for "Sensitive Compartmented Information." TOP SECRET//SCI clearance status is reserved for a subset of TOP SECRET clearance holders who have access to particularly sensitive government secrets. In order to be granted access to classified government information, Defendant

had to undergo an extensive background check process, sign documents indicating his understanding of his obligation to safeguard classified NDI, and have a demonstrated need to know the information in question. During his time with both CIA and DIA, Defendant signed multiple documents acknowledging the consequences of failing to protect classified information, including loss of access to such information, loss of employment, and criminal prosecution. *See, e.g.*, Government Exhibit ("GX") 1-1; GX 1-4 through 1-7; GX 2-3 through 2-9; GX 2-11 through 2-17.[3]

[3] The non-disclosure agreements that Defendant signed frequently included language such as the following:

> I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code.

See, e.g., GX 2-8, ¶ 8, GX 1-1, ¶ 7.

The multiple non-disclosure agreements that Defendant executed at multiple points in his career likewise warned that "the unauthorized disclosure of classified information by [Defendant] may constitute a violation, or violations, of United States criminal laws, including the provisions of" 18 U.S.C. § 794. *See, e.g.*, GX 1-1, ¶ 4; *see also* GX 1-8 (Defendant acknowledging receipt of DIA access suspension letter reminding Defendant of his "continued ·obligation to protect classified information, sensitive compartmented information, and intelligence sources and methods from disclosure to unauthorized or uncleared personnel under the provisions of Sections 793 and 794 of title 18, United States Code and/or the appropriate articles of the Uniform Code of Military Justice. **The time limit for safeguarding such intelligence never expires.**") (emphasis in original).

In addition to being put on notice repeatedly of the ramifications of failing to comply with his obligations to safeguard NDI, Defendant had experienced firsthand the negative consequences of violating the terms of his TOP SECRET security clearance. In 2010, while on administrative leave from DIA for performance-related issues, Defendant took a position with a cleared intelligence contractor without notifying his supervisor at DIA, as he was required to do. *See* Redacted DIA Office of the Inspector General ("OIG") Report of Investigation at p. 2, ¶ 7(c). ("OIG Report")[4] (Ex. A). While working for that contractor, Defendant disclosed classified information pertaining to the same assets, the "Johnsons," who were the subject of the documents referred to as Document No. 1 and Document No. 2 at trial. *See* Declaration of Robert Ambrose, dated Sept. 11, 2018, ¶¶ 3, 5 (Ex. B). Defendant denied passing any classified information to the outside contractor, whose employees he understood to have active TOP SECRET security clearances. *See* Redacted Affidavit of Kevin P. Mallory, dated Sept. 24, 2010, at 4 ("They both had TS clearances as I understood it.") (Ex. C).[5] As a result of this unauthorized disclosure of classified information to individuals who, while holding the requisite security clearance level, did not have a need to know, Defendant was stripped of his security clearance. *See* Redacted[6] Security

[4] The government attaches a redacted, unclassified version of the OIG report as Exhibit A to protect the classified equities therein. The Court has previously reviewed the classified version in the context of Classified Information Procedures Act ("CIPA") proceedings related to this case. *See* Exhibit L attached to Government's In Camera, Under Seal Notice of Objections Concerning Use, Relevance, and Admissibility of Classified Information Identified in Defendant's CIPA Section 5(a) Notice and Identification of National Defense Information Pursuant to CIPA Section 10, filed March 1, 2018 ("Gov't Mar. 1 CIPA Br.").

[5] The government is also providing as Exhibit C to this filing a redacted version of Defendant's declaration given as part of the 2010 OIG investigation. The unredacted version was previously provided to the Court as part of the CIPA proceedings in this case. *See* Exhibit L to Gov't Mar. 1 CIPA Br.

[6] The unredacted version was previously provided to the Court as part of the CIPA proceedings in this case. *See* Exhibit N to Gov't Mar. 1 CIPA Br.

Clearance Adjudication, dated Jan. 10, 2011 (Ex. D).[7]

Thus, Defendant knew that disclosure of information regarding the assets referred to as the "Johnsons" at trial had previously resulted in serious consequences for himself, even when that information was only revealed to United States' TOP SECRET security clearance holders. There could be no doubt in Defendant's mind, then, that the USIC took the protection of this type of information very seriously. Nonetheless, Defendant conspired to pass, passed, and attempted to pass information regarding the "Johnsons" to Chinese intelligence officers.[8] He did so knowingly and with a conscious disregard of his duties to not only his country, but also the former assets he handled, as is discussed further below.

The evidence adduced at trial showed that Defendant's primary motive was financial gain. At the time of the criminal conduct at issue, Defendant had not had steady income since his departure from his CIA contractor job in 2012. As of January 17, 2017, Defendant was $12,205.32

[7] During the course of his attempts to be reinstated from his administrative leave, Defendant also sent classified information through the United States mail. *Id.* at 2, § 2.a. This did not appear to be an inadvertent mishandling of such information as Defendant removed classification markings from the mailed documents prior to sending. *Id.* This is yet another example of Defendant's demonstrated disregard for his sworn duty to protect this country's national defense information.

[8] Documents Nos. 1 and 2 both pertained to a DIA operation involving the "Johnsons." The evidence at trial showed that Michael Yang received Document No. 1. *See, e.g.*, GX 8-6, Row 17; *see also* GX 8-18. FBI reverse engineering expert James Hamrock testified that within a minute of typing "Send 1" on May 5, 2017, Defendant transmitted a document from the CovCom device. *See* GX 8-21, p. 8; *see also* GX 8-6, Rows 84, 88, 92-93 (Yang requesting and Defendant stating he was sending Document No. 2). Special Agent Stephen Green testified that the redacted title in the chats corresponds to the classified title for Document No. 2, which was a classified PowerPoint discussing an operation utilizing the "Johnsons." (Testimony of Special Agent Stephen Green at pp. 595, 602, 609). The un-redacted version of the chats was provided to the Court during CIPA proceedings in this matter. *See* Exhibit V, Rows 25-29, 87-88, 92-93, attached to Government's Combined Motion Pursuant to CIPA Section 6(c) for Substitutions in Lieu of Disclosure of Classified Information, Motion for Protective Order Pursuant to Fed. R. Crim. P. 16(b)(1), and for Hearing on the Same, filed March 19, 2018.

.

past due on his mortgage payments, and Bank of America had consequently sent him a Notice of Intent to Accelerate his mortgage payments. GX 10-1. In addition to this mortgage debt, Defendant had over $30,000 in credit card debt at the time of his June 22, 2017 arrest, GX 10-8, as well as a Home Equity Line of Credit with a balance of $200,003.49 with a minimum payment of $4,582.47 due on February 16, 2017. GX 10-4.[9]

In sum, the history and characteristics of this Defendant reflect an individual who, despite understanding the consequences of his actions, was willing to betray his country, and to endanger the lives of human assets for nothing more than financial gain. Such history and characteristics counsel in favor of a sentence of life imprisonment.

2. *Nature and circumstances of the offense*

Defendant, who was entrusted with our nation's critical secrets, put our country and human lives—including the lives of assets—at risk for financial gain. He then lied about his actions and took steps to conceal them. Accordingly, the nature and circumstances of the offenses amply demonstrate why a sentence of life imprisonment is appropriate.

a. Defendant abused his prior position of trust for financial gain.

The sole reason that Defendant had access to classified NDI in the first place was the trust that the U.S. government placed in him. As a result of that trust, he was given access to classified documents and information relating to human assets, as well as to secret government programs. And as Defendant's nondisclosure agreements made clear (*see* note 4, *supra*), that grant of trust

[9] While Defendant's financial difficulties certainly provide a motive for why he would want to sell U.S. government secrets to Chinese intelligence officers, they do not in any way justify his conduct. Countless individuals across the country experience financial difficulties without turning to crime.

came with a **lifetime** obligation to protect our country. Nonetheless, Defendant betrayed that trust by conspiring to sell, selling, and attempting to sell NDI to the Chinese government. Defendant committed these crimes not by accident or on a whim, but through a calculated series of acts over the course of several months.

First, Defendant presented himself on social media in a way that would make it clear to foreign intelligence services that he had been a member of the USIC. Defendant said as much to CIA investigator Michael Dorsey in discussing his LinkedIn profile. *See* GX 7-31T (noting that, while his LinkedIn profile did not specifically state that, "I was an Intelligence Officer . . . anybody who has a refined eye sees those kinds of things"). Thus, it likely came as no surprise to Defendant that Chinese Intelligence Officers ("IOs") targeted him for potential recruitment.

Second, Defendant recognized that Michael Yang and "Mr. Ding" were likely Chinese intelligence officers but continued to engage with them. For example, the notes Defendant took about his Skype conversation with Michael Yang in late February 2017 included references to "Priv. and CG clients,"[10] "Focus – China/US relations," "wants to use public/private networks," and "Military matter related to China," among other things. GX 3-9.[11] Defendant also noted during his CIA interview that in his "judgment . . . these guys work for Chinese Intelligence, specifically targeting people outside of their country." GX 7-4T;[12] *see also* GX 7-8T ("the fact that they're asking this kind of stuff tells me…that they're probably in the Intel service"); GX 7-

[10] "CG" was plainly a reference to "Chinese Government" clients.

[11] Defendant acknowledged that the Chinese IOs seemed especially interested to see if he could get a job in the Trump administration. GX 7-12T ("every once in a while they asked me about that; well, have you heard anything, have you heard anything?"); GX 7-14T ("He emphasized to me that he hoped that I could get a job with, on the Trump Administration.").

[12] Defendant himself said that he had strong suspicions about these individuals being Intelligence Officers as early as his first trip to China in March. GX 7-9T.

40T ("And then they emphasized, at that point they said, you know, we really don't want academics. We want – and then they – they didn't use the word Jee Mee which is top secret of something. But they emphasized that it was not stuff that you could publicly get."); GX 7-41T ("my sense is that they were looking for Government secrets, U.S. Government secrets"). Defendant reiterated his belief that he was dealing with PRC intelligence during his subsequent FBI interview. *See, e.g.*, GX 13-3T ("Then we have Michael Yang who is, we'll say intelligence officer . . . and then there's a third Mr. Yang . . . Who is his boss."); GX 13-12T ("I actually contacted the Agency twice. When I first got – my first trip when I went over there and got kind of – the hair on my neck came up"); GX 13-13T ("it appears to me, based upon my experience... that they're either intel – either the intel s – one of the intel services there"); GX 13-14T ("they didn't use the, the Chinese, you know, the term secret or top secret…but they infer that they're looking – eventually looking for information that is, uhm, not, you know, our, our terminology, not open source").

Third, Defendant took aggressive steps to advance his relationship with the Chinese IOs to a point of personal profitability. He did this by traveling to the PRC on two separate occasions in March and April 2017 to make contact with the individuals he believed to be officers of a hostile intelligence service. On one of these visits, Defendant sent Michael Yang three unclassified documents, attached to an email with the subject line "Examples." *See* GX 3-18. One of those documents bore the CIA logo, and a second was a list of U.S. military acronyms and their definitions. *Id.* Former DIA Director of Operations, Michael Higgins, who served as the top-most human intelligence official at DIA, testified that provision of these materials followed the typical foreign intelligence service recruitment pattern. Mr. Higgins testified that a foreign IO will want proof that a potential U.S. asset has government access and that the documents Defendant sent

would be part of providing those bona fides. Testimony of H. Michael Higgins at pp. 35-37.

Fourth, having proven his bona fides by sending unclassified government documents and relaying whatever oral information he provided (information which is still unknown to the U.S. government), Defendant progressed to the stage of accepting money from the Chinese IOs. Over the course of two trips to the PRC, Defendant accepted $25,000 in cash, in addition to airfare, accommodation, and incidentals from officers working for a hostile intelligence service. These payments appear to have been solely for his travel to the PRC, provision of some *unclassified* U.S. government information, and whatever further information Defendant provided to the PRC Intelligence Services ("PRCIS") in person. Michael Higgins described the exchange of payment as a "watershed" event in an asset recruitment relationship. Testimony of H. Michael Higgins at pp. 38-39. Notably, these payments, which were not insignificant, pre-dated Defendant's transmission of the NDI at issue in this case.

Fifth, Defendant further advanced his plan to provide classified NDI to the PRC in exchange for payment by taking possession of a Samsung phone that he described as a "CovCom device." This device was provided by the IOs to facilitate secure communications and avoid government detection. *See* GX 13-16T ("I said . . . 'What keeps someone else from seeing what we're talking about?' He goes this phone would only work with this phone. Only these two. I said, 'So you mean, uh, like – your government or my government can't see what's in this phone.' He goes, 'No, only these two phones.'"). As FBI reverse engineer James Hamrock testified, the custom Chinese app loaded onto the CovCom was designed to automatically destroy communications, and it was likely only because of a fortuitous crash that some of Defendant's

prior chats with Yang were saved.[13] Those prior communications demonstrate how Defendant was willing to abuse his position of trust for financial gain. He told Michael Yang, "I have arranged for a USD account in another name. You can send the funds broken into 4 equal payments over 4 consecutive days. When you agree I will send you the bank I.g instructions." GX 8-6, Row 46-47; *see also*, GX 8-6, Row 134 ("I have a account not in the US you can send it to and I have the means to move it from there.").

Sixth, Defendant took the most substantial step of all in his calculated scheme to exchange NDI for cash by digitizing NDI in his possession. On April 25, 2017, Defendant entered a Leesburg, Virginia FedEx store to scan eight classified government documents and a classified table of contents to a micro SD card that was compatible with the CovCom device. These were documents Defendant had retained since leaving government service – some documents dating back to as early as 2009. And yet, it was only in 2017, after receiving initial payments of $25,000 from the PRCIS and hoping to earn even higher payments,[14] that Defendant digitized them. It was only when Defendant had a potential payday lined up, that he loaded these documents into the CovCom device for transmittal to a hostile foreign intelligence service.

And transmit he did, as the evidence at trial showed. *See* GX 8-21 (log files showing send

[13] While *some* of Defendant's communications with Michael Yang were visible on the device, there were undoubtedly more that the FBI could not recover. For example, the first communication that was visible in GX 8-6 was dated May 1, 2017. However, the device was customized for Defendant's use beginning on April 14, 2017, the same date that he arrived in China for his second trip. GX 8-28 (Hamrock overview of log files showing alterations to CovCom device to enable secure communications). There almost certainly had to be communications that occurred when Defendant was trained on how to use the device while he was in the PRC. Given that those communications were not recoverable, there is no way to know what *other* communications Defendant had on the device that were also not accessible to the U.S. government.

[14] Defendant's reference in GX 8-6 to breaking the money into four separate payments certainly indicates that he expected to receive some large payments. Structuring the money that way would potentially allow him to avoid raising any suspicion by ensuring that any individual financial transaction did not exceed $10,000.

sequences for multiple classified documents); GX 8-18 (WeChat chart showing receipt of Table of Contents and Document No. 1 by Michael Yang's WeChat account on May 1, 2017).[15] Defendant's own words confirm that Defendant had continued his methodical engagement of the Chinese IOs by transmitting and attempting to transmit information regarding U.S. government intelligence "targeting." *See, e.g.*, GX 8-6, Rows 31-33. Defendant's own words demonstrate that, in the final phase of his painstaking plan to maximize his financial gain, Defendant intended to provide information about U.S. government targeting operations – information that would be incredibly valuable to the Chinese and incredibly damaging to the U.S. government[16] – for the right price. Defendant's aim was clear: to prolong the relationship so that he could make as much money as possible. Defendant's criminal course of conduct required that he would sell as much NDI as he could, for as long as he could, regardless of the consequences for our country's and our assets' safety. *See, e.g.*, GX 8-6, Row 51 ("I will send more docs when payments are made."). His plan ended only because of the FBI's successful efforts in discovering and disrupting Defendant before he could cause even more damage to the national security of the United States.

All of these steps show Defendant was calculating in his engagement with the PRCIS in 2017. Defendant used his former security clearance to take such steps. This is a Defendant who

[15] Because Defendant was convicted of an ongoing conspiracy to transmit NDI to the PRCIS, it would be far too narrow to focus solely on the two documents – the handwritten Table of Contents and Document No. 1 – that Michael Yang demonstrably received. Defendant engaged in far reaching conduct involving at least eight classified national defense documents. Further, it bears repeating once more that Defendant spent hours meeting with PRCIS officers and very well may have passed additional classified facts either orally or in writing while in the PRC.

[16] While the defense attempted to claim at trial that the information that Defendant provided was essentially worthless, that claim is belied by the fact that these Chinese IOs had already paid Defendant $25,000 before we can show any classified documents were passed, they provided him with a CovCom device to ensure the secure passage of classified information, and they were planning to have him travel to China for a third time. GX 8-6, Row 140 ("If you think the situation is ok and you're available, you may still come in mid June)." This claim was also soundly rejected by the jury.

abused his position of trust for financial gain. He had no higher principle than a desire to make as much money as possible from the classified information that he was never authorized to have once he left U.S. government service.

b. Defendant jeopardized actual human assets

One of the most troubling aspects regarding the nature and circumstances of these offenses is the fact that Defendant jeopardized the safety of actual human assets. Despite the defense's attempt to downplay the impact of the information Defendant conspired to send, sent, and attempted to send to Michael Yang, the evidence at trial highlighted the sensitivity of this NDI. DIA witnesses Robert Ambrose and Michael Higgins both testified that the DIA documents contained information about a human asset operation. *See also* Declaration of Max Mikel Kingsley, Chief, Oversight and Compliance, Directorate for Operations, Defense Intelligence Agency at ¶¶ 8-9, Ex. G to Gov't Mar. 1 CIPA Br. Mr. Higgins, in particular, noted that the "net of suspicion" is cast wide when an asset is compromised – meaning not only are the assets put at personal risk, but so too are any known associates of those assets. Testimony of H. Michael Higgins at p. 26.

Similarly, CIA Original Classification Authority ("OCA") Nancy Morgan testified that Document No. 4, entitled "Foreign Country A Intelligence Service Capabilities #4" also dealt with sensitive human asset operations. Defendant attempted to send this document *four separate* times on May 1 and 2, 2017. Defendant also attempted to send a second document, captioned "Foreign Country A Intelligence Service Capabilities (B) #5" one time on May 2, 2017. *See*, Ex. E

(demonstrative exhibit used by the government during rebuttal closing); GX 9-3E5.[17] Ms. Morgan testified that this document, *also related to human assets*, was the most sensitive of the CIA documents found in Defendant's home. Ms. Morgan testified that the CIA documents contained cryptonyms, that is, information about real people who could be put at real risk by Defendant's actions. Testimony of Nancy Morgan at p.p. 796-802. *See also* Dkt. 25-1, Declaration of Antoinette B. Shiner, July 7, 2017 ("July 7 Shiner Decl."), ¶ 6 ("The CIA information contained in the documents at issue reveals a broad range of sensitive national security related information, to include sensitive intelligence collected by the CIA, the CIA's analysis of the intelligence it collected, and in some instances, the actual sources of the intelligence, which range from human sources to technical collection."); *see also* Declaration of Antoinette B. Shiner Information Review Officer for the Litigation Information Review Office Central Intelligence Agency, Paras. 11-12, 14-15, Exhibit A to Gov't Mar. 1 CIPA Br.

Most troubling of all, Defendant sent the information about the DIA human assets *after* he learned that those assets would be traveling to the PRC in the summer of 2017. *See* GX 3-26 (Defendant's LinkedIn chats with the "Johnsons"). Defendant attempted to renew his relationship with the "Johnsons" at precisely the time that he was meeting with Chinese intelligence officers for hours-long meetings over multiple days in Shanghai. Defendant sent the "Johnsons" one short LinkedIn message in 2013, more than two years after resigning from DIA. GX 1-13. There was no communication in 2014 or 2015 with the "Johnsons," and the only communications in 2016 were messages from Defendant on March 7th, March 21st, and September 26th with the same content – "Congrats on the anniversary! Hope you're doing well." *Id.* However, between March

[17] The naming conventions for these two documents, as well as for a number of other documents in Defendant's hand-written table of contents, were edited to avoid disclosing classified information following CIPA proceedings in this case.

28th and March 29th – just over a week after Defendant's first trip to the PRC to meet with Michael Yang and Mr. Ding – Defendant sent the "Johnsons" *nine* LinkedIn messages. In one of those messages, Defendant informed the "Johnsons" that he had "been traveling to China lately for some consulting work." He then asked, "Do you have any interest there that I can help you with please let me know?" *Id*.

Chillingly, "Mrs. Johnson" told Defendant that she and her husband would be traveling to the PRC that summer. *Id.* Just a few weeks later, Defendant sent Document No. 1, containing information about the work the "Johnsons" had done with DIA to the Chinese. A few days after that, Defendant completed the steps needed to transmit Document No. 2, which contained even more detailed identifying information about the "Johnsons." *See* GX 8-21; GX 8-6, Row 88 and 93. Fortunately, the "Johnsons" were able to travel to and from the PRC without incident, but that does not change the fact that Defendant knowingly put them at grave risk while they were there.[18]

c. Defendant took multiple steps to evade detection and thwart a criminal investigation.

While Defendant was convicted in Count Four of making two materially false statements to FBI special agents, his lies in the course of this investigation were much more expansive than that. During the border search in Chicago in April, Defendant told at least two blatant lies. He first lied on the Customs form when he checked "No" in answer to the question, "I am carrying currency or monetary instruments over $10,000 U.S. or foreign equivalent," even though he was carrying approximately $16,500 in cash. GX 5-1. Defendant also lied about the CovCom device,

[18] Given this conduct, Defendant cannot credibly claim to deserve a downward departure under Application Note 2 to USSG § 2M3.1, which only permits a downward departure where revelation of the information at issue would likely cause "little or no harm." In this case, revelation of this information could potentially have caused the greatest harm of all – the death of U.S. intelligence assets.

telling the CBP agents that this Samsung phone was a gift for his wife.

Four days after telling those lies to the Customs officers in Chicago, Defendant went to the FedEx store closest to his home and saved eight classified U.S. government documents to a micro SD card. He then paid to have those documents shredded, GX 6-4, a fact which he confirmed when he told Michael Yang, "I already destroyed the paper records. I cannot keep these around…too dangerous." GX 8-6, Row 81.

When he was interviewed at the CIA approximately two weeks later on May 12th, he lied to Mike Dorsey repeatedly. When Mr. Dorsey asked if he was supposed to be collecting printed research or writing a paper for these Chinese IOs, Defendant merely said, "[s]o it wasn't clear." GX 7-16T; *see also*, GX 7-20T (Dorsey: "Did you send them anything on that phone?" Defendant: "I sent them some tests of some sort, just to see if I could do it right. And I couldn't figure it out"); GX 7-21T (Dorsey: "What were the tests?" Defendant [following a very long pause]: "It was something innocuous. It was an image. It was some typed something"); GX 7-23T (Dorsey: "So how many communications have you had with Michael on the . . . Samsung?" Defendant: "One time"); GX 7-42T (Dorsey: "Did you put something in writing for them?" Defendant: "No.").

When he was interviewed by the FBI at the hotel in Ashburn, just 12 days after that, the lying continued. *See* GX 13-10T (SA Green: "So have you written papers for them?" Defendant: "I think two or three paragraphs. But I wrote it right there in country . . . I just typed it right there, uh, in the business, uh, you know, business office"); GX 13-11T ("I've tried to s-send a message, practicing with them, but I haven't been successful"); GX 13-25T (SA Green: "so you, you wrote them a couple of papers. Did you give them any other documents?" Defendant: "No.").

The Defendant was almost certainly willing to meet with the FBI for hours, and to lie to them repeatedly, precisely because he so firmly believed that the CovCom device was secure. *See*

GX 7-18T ("[A]s I recollect, your conversations don't sit in forever. They kind of, after a period of time, it kind of just dies away"); GX 7-19T ("When you do that you're in the system . . . Now we can, we can talk, so to speak clearly; in the clear; securely"); GX 7-22T ("So if someone did intercept them, they couldn't do it . . . Because the encryption is so stiff"); GX 13-17T ("So it's encrypted"); GX 13-19T ("Now I don't know if I have conversations anymore . . . Because they – they fall away after . . . some length . . . I go back in and it's, it's gone").[19]

Following that May 24th interview, Defendant was very much on notice that the FBI knew a good deal about his activities with these Chinese IOs because the CovCom device had given him away. Not surprisingly, the evidence in this case showed a defendant who went to great lengths to conceal his criminal activities. As noted previously, the handwritten notes that he took when he was trained on the CovCom device, GX 8-17, were never found despite a very thorough search of Defendant's house. In addition, after the Ashburn hotel interview, the WeChat application from the CovCom device was deleted, undoubtedly by Defendant. He must have deleted it almost immediately after the FBI interview, because he contacted Michael Yang by email on May 26th (two days after the FBI interview) to tell him, "Pls send my ur SKYPTE. I am having problems with WeChat." GX 3-22.

The WeChat application was not all that he deleted. Both a Kingston Micro SD card and a MacBook Pro computer were found in Defendant's house on June 22nd. Filenames for the eight classified documents that were later found on the Toshiba Micro SD card were recovered from the Kingston Micro SD card, but only from the deleted space. GX 9-8B. In addition, log files from

[19] Further demonstrating Defendant's belief that the CovCom device was secure, when he saw, to his surprise, that messages were visible on the device on May 24th, he told the FBI agents, "I'm surprised it kept this much. 'Cause I – it must have some limit or something." GX 13-22T*; see also* GX 13-24 ("I mean there's some other stuff, but – it's, uh, it's also stuff has disappeared on me. So that's why I thought maybe it has some limitation").

the MacBook Pro computer corresponded with the same naming convention as the eight documents from the Kingston Micro SD card.[20] Yet while the classified documents on the Kingston Micro SD card were recoverable, nothing else could be captured from the MacBook Pro computer beyond those log file names. This becomes more understandable given that the FBI located evidence of Defendant sending himself a link on April 24, 2017, the day before he went to the Fed Ex store, with the following URL, http://osxdaily.com/2013/06/09/secure-remove-files-directories-from-mac-os-x-with-the-command-line/. GX 3-16-1. Pasting that URL into a web browser pulls up an article that begins, "Need to securely delete a file, group of files, or an entire directory, insuring that it's quite literally never recoverable by any known possible means. You can do this easily. . . ." GX 3-16-1A.

During the search of Defendant's home, the Kingston SD card and the MacBook Pro computer were not concealed. However, the Toshiba Micro SD card on which the eight classified documents were saved, with logical filenames, was very carefully hidden inside of a drawer within Defendant's bedroom closet. It was only after a second sweep through that closet by FBI SA Melinda Capitano, a seasoned, former drug investigator, that the SD card was located. It was tightly wrapped in a ball of aluminum foil. GX 9-3A.

The importance of this item to Defendant became readily apparent, when, on June 24, 2017, he called his family from the Alexandria Detention Center on an open phone line, and enlisted his wife and his son to try to find the SD card. He spoke to his wife in Mandarin Chinese in part of

[20] The naming conventions on both the Kingston SD card and the MacBook Pro computer reflected the naming convention that the scanner in the FedEx gave the eight documents on April 25th. For example, the first filename on both GX 9-8B and GX 9-11 is 20170425155910 with "2017" reflecting year, "04" reflecting month, "25" reflecting day, and "155910" reflecting the time on a 24-hour clock which corresponds to 3:59 PM, the time that Defendant could be seen inside the FedEx store on April 25th. *See* GX 6-9, FedEx video surveillance footage.

the conversation, and told her to talk to his son about what they were looking for, but not to say the words aloud. GX 11-2T at pp. 3-5.

Simply put, the nature and circumstances of this offense weigh heavily in favor of a severe sentence. This was a defendant who was willing to betray his country for financial gain and willing to endanger the "Johnsons'" lives for financial gain. He repeatedly lied about his conduct, and was even willing to enlist his wife and his son into his attempts to thwart the FBI's criminal investigation and to conceal his activities.

3. *Reflection of seriousness of crime and deterrence of future criminal conduct*

The conspiracy offense that the jury convicted Defendant of, specifically the violation of 18 U.S.C. § 794, is among the most serious crimes in the Federal Code. This reflects a considered judgment on the part of Congress to forcefully punish individuals who betray this nation. Therefore, the statutory penalty is up to life in prison, and if "the offense resulted in the identification by a foreign power . . . of an individual acting as an agent of the United States and consequently in the death of that individual," this is a death eligible offense. Defendant's punishment should reflect how serious this crime truly is.

The Guidelines also reflect the seriousness of this offense, as evidenced by the fact that Defendant's Guidelines sentence is life in prison, even though Defendant has a Criminal History Level of I. Simply put, these are serious crimes that deserve a serious punishment of life imprisonment. A second reason that Defendant should be sentenced to life in prison is for purposes of deterrence, both general and specific. As to specific deterrence for this defendant, a severe sentence where Defendant's communication privileges are restricted is the only way to ensure that he will not attempt to convey the classified NDI in his head to the Chinese government.

As for general deterrence, there are millions of current and former security clearance

holders in this country, which include full-time government employees as well as government contractors. They all enter into similar non-disclosure agreements to the ones Defendant signed over the course of his career. Fortunately, the vast majority of clearance holders uphold those obligations faithfully. Yet for anyone considering violating those agreements, as Defendant did, there should be a powerful message sent that selling our secrets to a foreign adversary will be met with the harshest of punishments. A lifetime term of imprisonment in this case also serves to remind all clearance holders that the need to safeguard government secrets and protect the national security is a lifelong obligation.

4. *Avoidance of unwarranted sentencing disparities*

A final sentencing factor to consider is the "need to avoid unwarranted sentencing disparities among defendants with similar records who have been found guilty of similar conduct." 18 U.S.C. § 3553(a)(6). A review of similar cases reflects the fact that espionage convictions are dealt with seriously, and defendants who commit those offenses serve long jail terms.

United States v. Brian Patrick Regan, 1:01-CR-405 (E.D. Va. 2003) (Lee, J.), involved a defendant in the Eastern District of Virginia convicted of violations of 18 U.S.C. § 794. Regan was a member of the U.S. Air Force who, between mid-1999 and August 2001, while working at the National Reconnaissance Office, obtained classified intelligence related to the military preparedness of Iran, Libya, Iraq, and the People's Republic of China. Regan attempted to sell this TOP SECRET information to Iraq, Libya, and the PRC. *United States v. Regan*, 228 F. Supp. 2d 742, 745 (E.D. Va. 2002). Following his conviction at trial for two counts of attempted espionage in violation of § 794(a) and one count of obtaining information respecting the national defense of the United States with intent to cause injury to the U.S. and advantage to a foreign country in violation of 18 U.S.C. § 793(b), Regan was sentenced to life in prison. *See*, Judgment

in a Criminal Case at p. 4, Attached as Ex. F. This life sentence represented a sentence within the guidelines. Like the Defendant, Regan had an offense level of 46 and a criminal history category I, as a result of the same two enhancements that should apply in this case: one for abuse of a position of trust, USSG § 3B1.3, and one for obstruction of justice, USSG § 3E.1. *See* Sentencing Agreement at p. 2, Attached as Ex. G.

United States v. Pitts, 973 F. Supp. 576 (E.D. Va. 1997) (Ellis, J), involved another defendant in the Eastern District of Virginia, a former FBI agent, who was convicted of the same offense as Kevin Mallory – two counts of 18 USC § 794 – and who plead guilty to those offenses. *Id.* at 576-77. Pitts "betrayed his country by becoming an agent of the KGB," and by passing "unclassified and classified material to his KGB and SVRR 'handlers,'" for which he was paid at least $129,000. *Id*. at 577-78. Pitts was also the subject of a "false flag" operation[21] where he provided additional information to those he believed to be Russian contacts, but who were, in fact, "undercover FBI agents pretending to be SVRR officers." *Id*. at 578.

The Court found that the Guideline range for Pitts was 262-327 months, and sentenced him to near the top of that range – 324 months in prison. *Id.* at 584. In imposing sentence, the Court noted that Pitts had abused a position of trust because he was "a supervisory special agent of the FBI" and "a foreign counterintelligence operative." *Id*. at 583.

Defendant in this case enjoyed a similar position of trust. He was a former CIA and DIA case officer who interacted with sensitive human assets. He was entrusted with our nation's most sensitive secrets, and he betrayed that trust. As this Court noted in sentencing Pitts, his rationalizations for committing those offenses were "indefensible; none abrogates Pitts's moral

[21] A false flag operation is this context is when a criminal target is engaging with an undercover law enforcement officer posing as a member of a foreign intelligence service.

and legal duty not to betray his country." *Id*. at 585. The same could be said of this Defendant. He committed an indefensible crime, and he deserves a serious punishment for doing so. And unlike Pitts, Defendant did not accept responsibility for his crime through a guilty plea.

In *United States v. Hoffman*, 2:12-cr-184 (E.D. Va. 2014) (Doumar, J.), the defendant, a former cryptologic technician with the U.S. Navy, divulged classified information to undercover FBI agents posing as Russian intelligence officers after expressing his desire to be compensated in the form of job assistance or payments. In response to undercover agents' questions, Hoffman provided written responses that contained NDI classified at the levels of SECRET and TOP SECRET/SCI. Following a five-day trial, a jury convicted Hoffman of one count of attempted espionage, in violation of § 794(a). Under USSG § 2M3.1, Hoffman's offense level was 42, which resulted in a guidelines range of 360 months to life imprisonment. Hoffman was sentenced to 360 months in prison.

Defendant's criminal conduct is no less serious than that of Regan, Hoffman, and Pitts. Defendant passed information classified at the SECRET and TOP SECRET levels to Chinese IOs in exchange for cash. Defendant also conspired to pass additional, highly sensitive NDI that would have done grave damage to our nation's security. And perhaps most troublingly, disclosure of Document No. 2, which Defendant completed the send sequence to transmit, would have jeopardized the lives of human assets.[22] The government did not charge Defendant with successfully passing Document No. 2 in light of Michael Yang's text message to Defendant stating that Michael Yang had not been able to receive that particular document.[23] However, given

[22] Defendant also completed send sequences for Documents Nos. 4 and 5, which contained information regarding CIA assets in Foreign Country A. *See* GX 8-21. Defendant attempted to send Document No. 4 *four separate times*. *Id.*

23 Even though Defendant was not charged with successful passage of Document Number 2, he was charged, and convicted of a Conspiracy Count in Count One of the Indictment

Defendant's multiple attempts to transmit Document No. 2, there is reason to believe that he would have eventually succeeded in delivering this document to Chinese IOs if the FBI had not disrupted his scheme. Moreover, Defendant had hours of in-person meetings with Chinese IOs while he was in the PRC, for which he was paid. Although the government does not know what information Defendant provided during these meetings, reasonable inferences suggest that he likely provided the IOs additional NDI.

Accordingly, and against the backdrop of the serious sentences received by the defendants in *Pitts*, *Regan*, and *Hoffman*, a guidelines sentence of life imprisonment avoids unwarranted sentencing disparities.

III. CONCLUSION

For the foregoing reasons, the government respectfully requests that this Court sentence Defendant to the recommended sentence under the Guidelines: a term of imprisonment for life. That sentence not only comports with the USSG calculation, but also appropriately reflects the seriousness of the offense and the great risk of harm Defendant created not only for this country, but also for specific human assets who selflessly put their own safety at risk for the protection of the United States' national defense.

Dated September 14, 2018

Respectfully submitted,

G. Zachary Terwilliger
United States Attorney

By: /s/ Jennifer K. Gellie
JENNIFER KENNEDY GELLIE
Trial Attorney
National Security Division
United States Department of Justice
950 Pennsylvania Ave., NW

where his multiple attempts to transmit Document Number 2 were alleged as overt acts in furtherance of the conspiracy. *See*, Indictment at p. 13, Para. 20, 22-23.

Washington, D.C. 20530
Tel.: (202) 233-0785
Fax: (202) 233-2146
Jennifer.Gellie@usdoj.gov

JOHN T. GIBBS
COLLEEN E. GARCIA
Assistant United States Attorneys
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700
Fax: 703-299-3981
John.Gibbs@usdoj.gov
Colleen.E.Garcia@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that I have caused an electronic copy of the *GOVERNMENT'S POSITION WITH RESPECT TO SENTENCING* to be served via ECF upon counsel for Defendant Kevin Patrick Mallory.

By: /s/

John T. Gibbs
Virginia Bar No. 40380
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700
Fax: 703-299-3981